

The background of the slide is a blue-tinted photograph of a person rappelling down a rope against a cloudy sky. The person is wearing a helmet with a cross symbol and a vest with the word "SHERIFF" on the back. The text "Atlas" is overlaid on the image in a large, white, sans-serif font, and "Going Beyond the Public Safety Use Case" is overlaid below it in a smaller, white, sans-serif font.

Atlas

Going Beyond the Public Safety Use Case

Michael Ogata
NIST, Applied Cybersecurity Division

#PSCR2019

DISCLAIMER

Certain commercial entities, equipment, or materials may be identified in this document in order to describe an experimental procedure or concept adequately.

Such identification is not intended to imply recommendation or endorsement by the National Institute of Standards and Technology, nor is it intended to imply that the entities, materials, or equipment are necessarily the best available for the purpose.

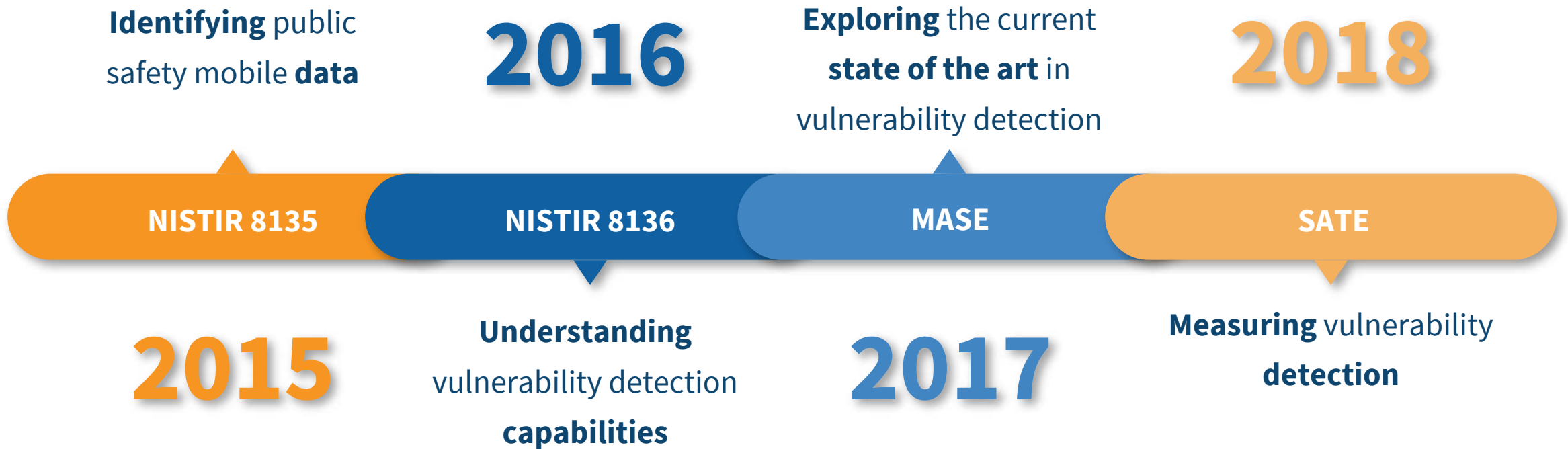
*Please note, unless mentioned in reference to a NIST Publication, all information and data presented is preliminary/in-progress and subject to change

Agenda

- The Road to Atlas
- Overview of Atlas' Purpose and Goals
- Advantages to the Approach
- Roadmaps and Future Huddles



PSCR Mobile App Security Work



A Common Problem: Framing Public Safety's Needs

Mobile Apps Are More than Just Smart Phone Apps



*In order to determine **how** to secure public safety mobile apps, we first have to determine **what** the apps do*

***What** apps do is tied to the **activities** Public Safety **engages in**.*

*The **activities** an app models will dictate the **information** handled by that app.*

Atlas Goals

Functions

Information Type Catalog

- High level descriptions
- Security Categorizations
- Links To Information Type Resources

Use Case Catalog

- Information Types in Context

Searchable Resource

- Keyword
- Types
- Disciplines



Audience

Public Safety

- Increased understanding of threat landscape
- Seeing activities through the lens of Cybersecurity

App Developers

- Better informed
- Protocols
- Best Practices

Anatomy of a Use Case

Apps model Actions, Actions require Information



Who

What

Where

Anatomy of a Use Case

Apps model Actions, Actions require Information



Who

Actors

- Responders
- Victims
- Witnesses
- Suspects

Disciplines

- Fire
- Law Enforcement
- EMS

Organizations

- State Police
- Highway Patrol

Anatomy of a Use Case

Apps model Actions, Actions require Information



Who

Hazards

- Weather
- Chemicals
- Weapons

Technologies and Assets

- Radios
- Wearables
- Sensors

Activities

- Triage
- Traffic stop
- Containment

Anatomy of a Use Case

Apps model Actions, Actions require Information



Who




Event Location

- Urban/Rural
- Interior/Exterior
- Suspects

Responders

- GPS
- Floor
- Geofencing

Use Case Information Security Categorization

	Low	Moderate	High
	Low	Moderate	High
	Low	Moderate	High

Adverse Effects

Operations



Assets



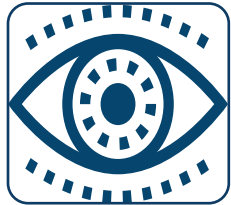
Individuals



Reputation



Use Case Information Security Categorization



Low

Low

Low



Who

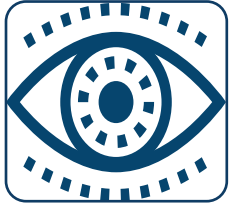


- **Responder**

- Name
- Rank
- Organization

...se to a
...efighter
...s/her
...navigate
...ing as well
...ter location
...t

Use Case Information Security Categorization



Low

High

High



Who



- Building Schematics
- Vital Readings
- Responder Location

...ponse to a
...firefighter
...n his/her
...to navigate
...building as well
...fighter location
...dent

Atlas Use Case Catalog

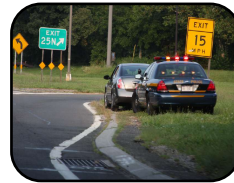
- Collection of Use Cases
- Searchable
 - Discipline
 - Info Type
 - Keyword



Building Fire

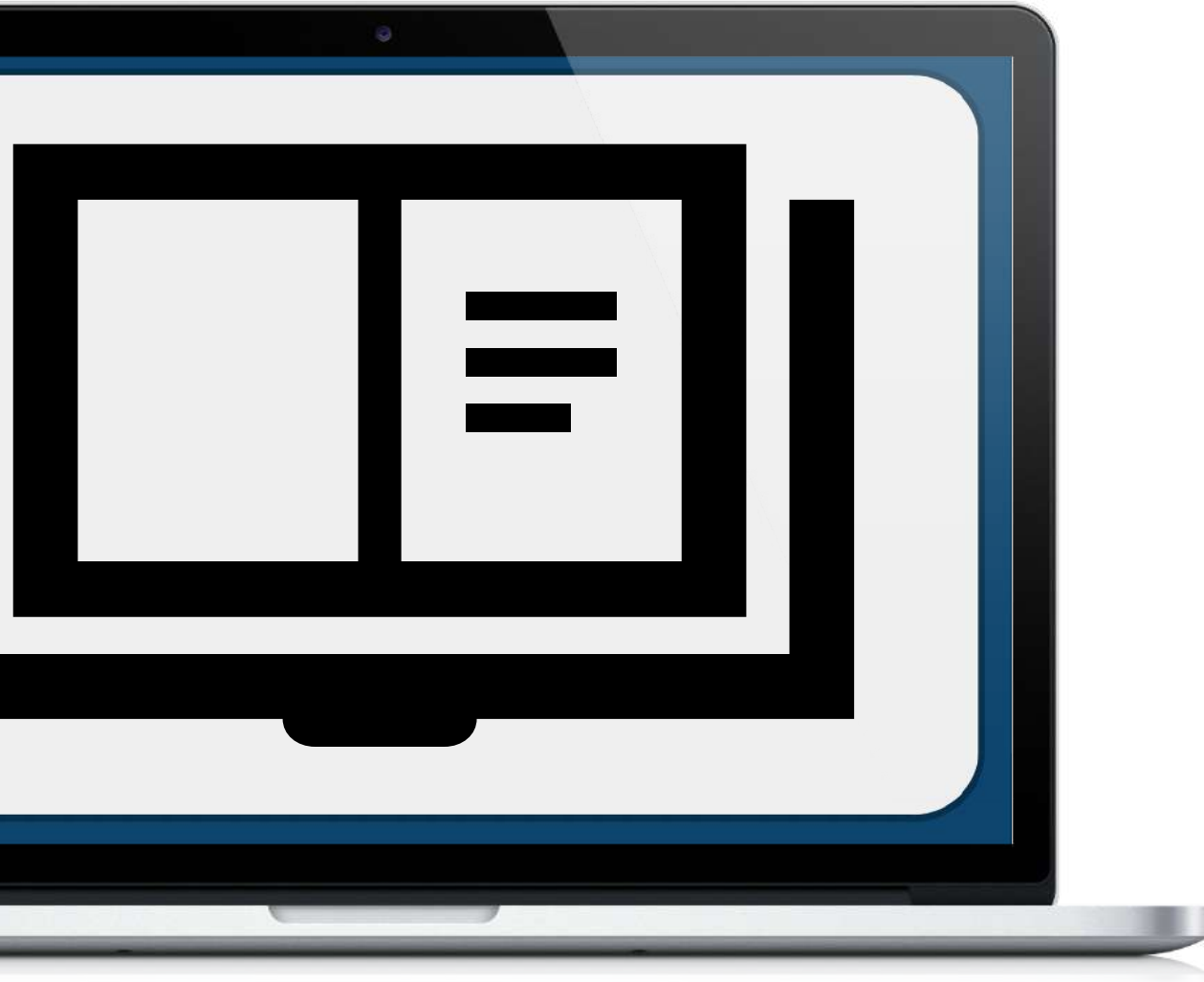


Cardiac Arrest



Traffic Stop

Atlas Information Type **Catalog**



- Collection of Information Types
- Searchable
 - Keyword
 - Security Categorization
- Cross reference against Use Cases
- Maps types to resources

Atlas Target Audience

Benefits and Uses



First
Responders



Information
Security
Officers



App
Developers



Public
Safety
Researchers

NIST Cybersecurity Framework



Framework Core

Identify

Asset Management
Governance
Risk Assessment

Protect

Identity
Management
Authentication

Detect

Event Detection
Continuous Monitoring

Respond

Planning
Mitigation
Analysis

Recover

Planning
Improvement
Comms

Vital Readings



Low

High

High

Atlas Target Audience

Benefits and Uses



First
Responders



Information
Security
Officers

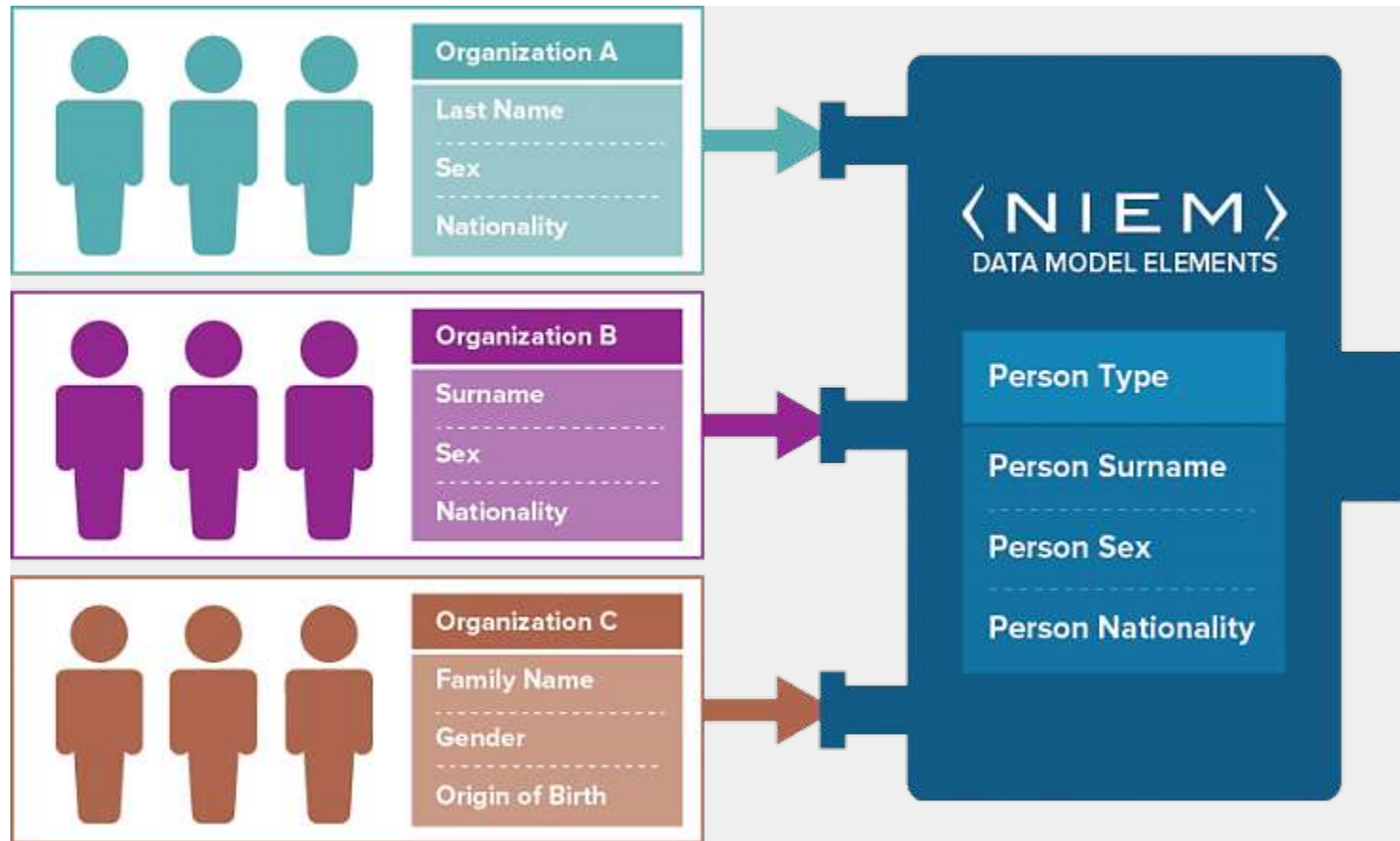


App
Developers

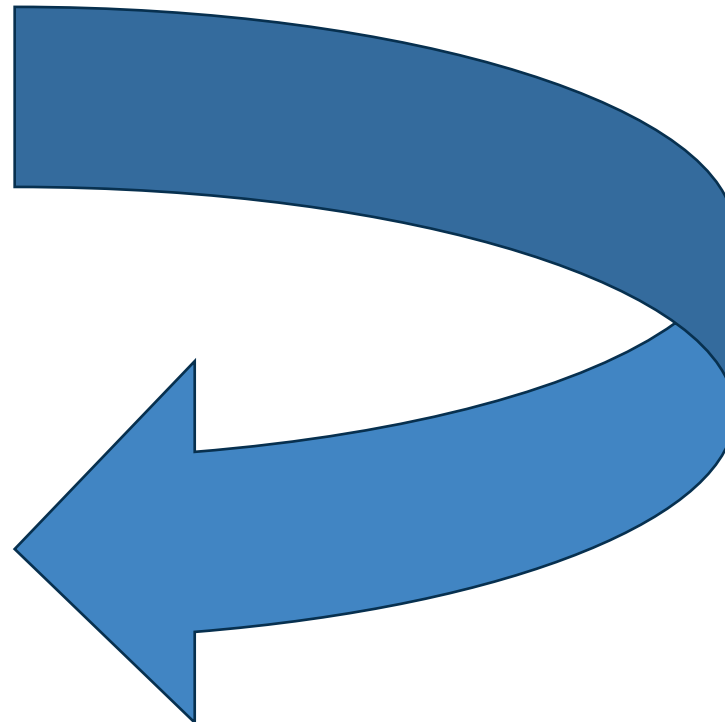
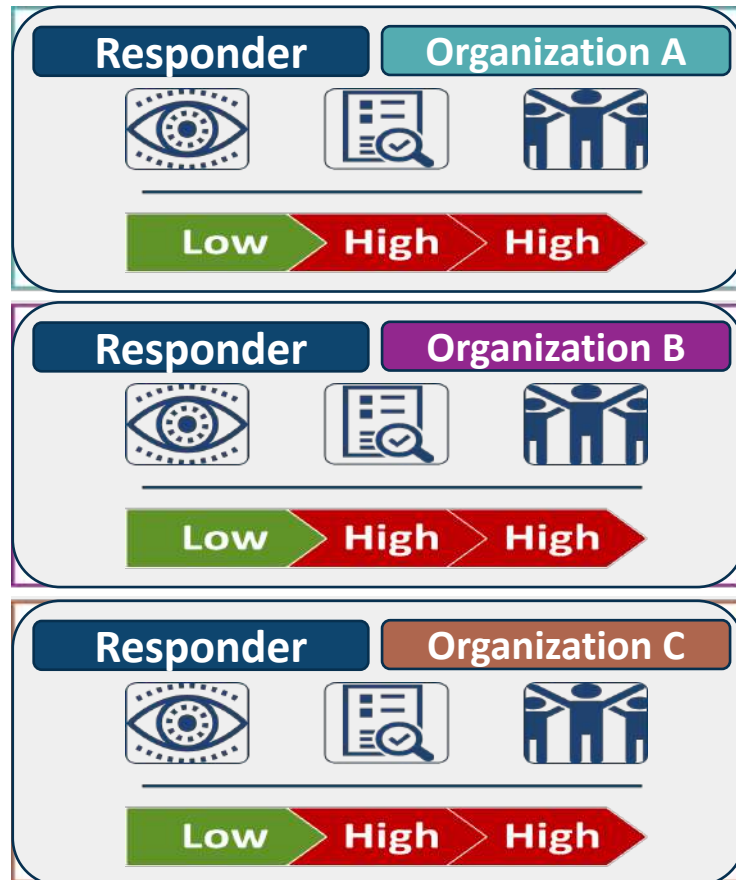


Public
Safety
Researchers

NIEM – National Information Exchange Model

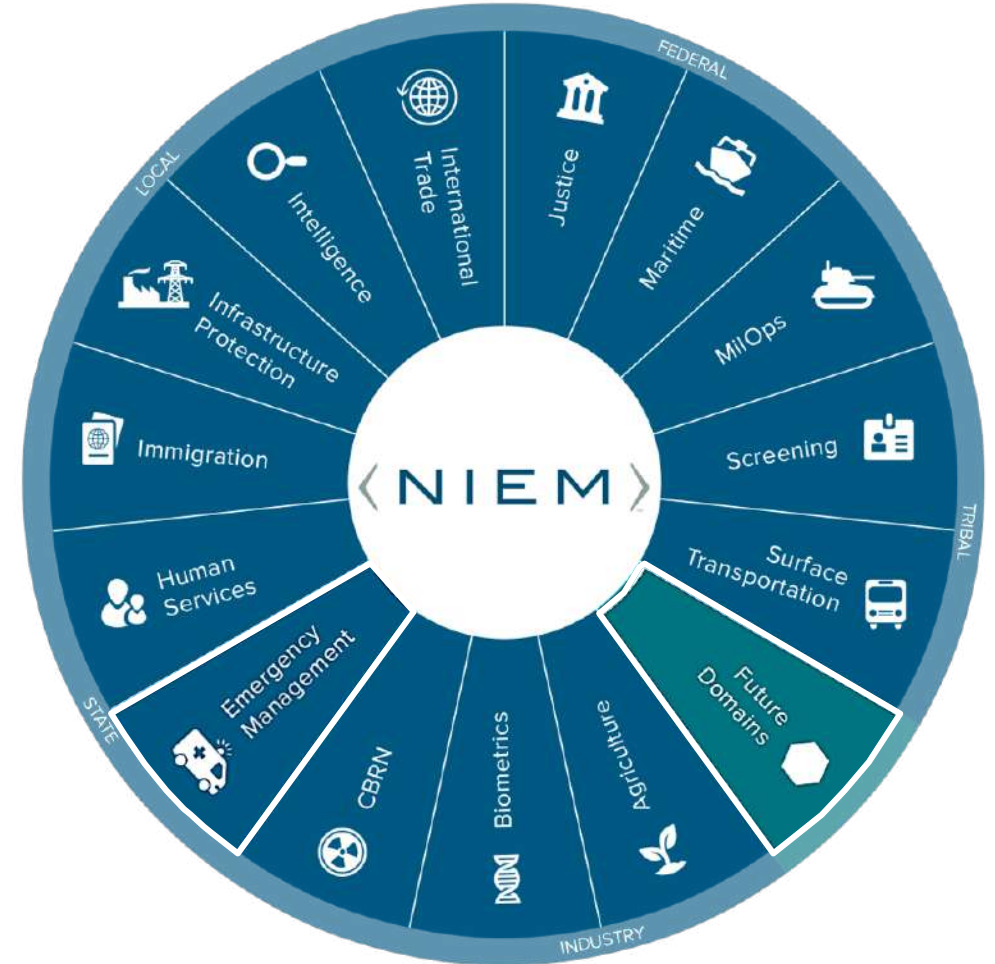
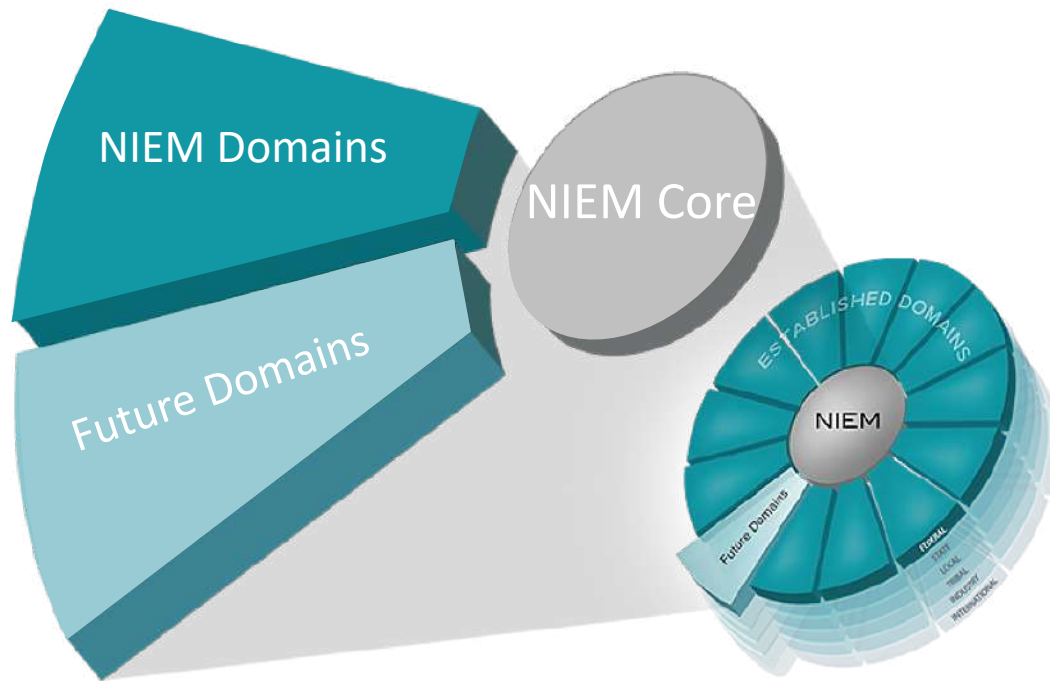


NIEM – National Information Exchange Model



```
"nc:PersonFullName":{  
  "description":"A complete name of a p  
  "$ref":"#/definitions/nc:PersonNameTe  
},  
"nc:PersonGivenName":{  
  "description":"A first name of a pers  
  "$ref":"#/definitions/nc:PersonNameTe  
},  
"nc:PersonMaidenName":{  
  "description":"An original last name  
  "$ref":"#/definitions/nc:PersonNameTe  
},
```


NIEM – National Information Exchange Model



Atlas Target Audience

Benefits and Uses



First
Responders



Information
Security
Officers

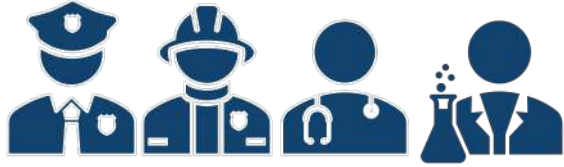


App
Developers



Public
Safety
Researchers

Public Safety Research

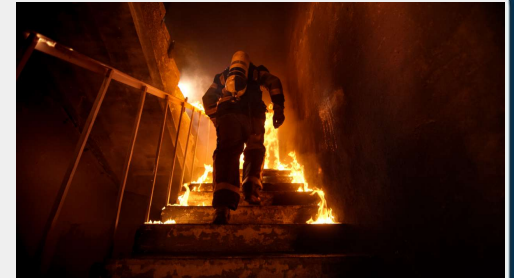


- Common description of public safety activities
- Enables collaborative research efforts
 - Identity management
 - Usability
 - Interoperability

Who

What

Where



During a response to a building fire, a firefighter uses an app on his/her mobile device to navigate through the building as well as provide firefighter location to the fire incident commander.

Hurdles and Future Work

- Expand the use case database
- Export/link to use case data into NIEM schemas
- Expand information type links resources
- Looking for feedback – check out the demo!



Michael Ogata
NIST, Applied Cybersecurity Division
michael.ogata@nist.gov

THANK YOU

Security for First Responder Mobile and Wearable Devices

Gema Howell

NIST, Applied Cybersecurity Division

Presentation Overview

- Mobile and wearable devices identified
- Purpose of the project
- Project outline
- Public safety security objectives
- Mobile and wearable test analysis
- Best practices and guidance

Mobile and Wearable Device Examples



The Why

- More Devices, More Problems
- First Responders are/will use mobile and wearable devices to achieve their daily life saving activities
- The security of these public safety devices are important to ensure minimal impact on their daily activities

Project Goals:

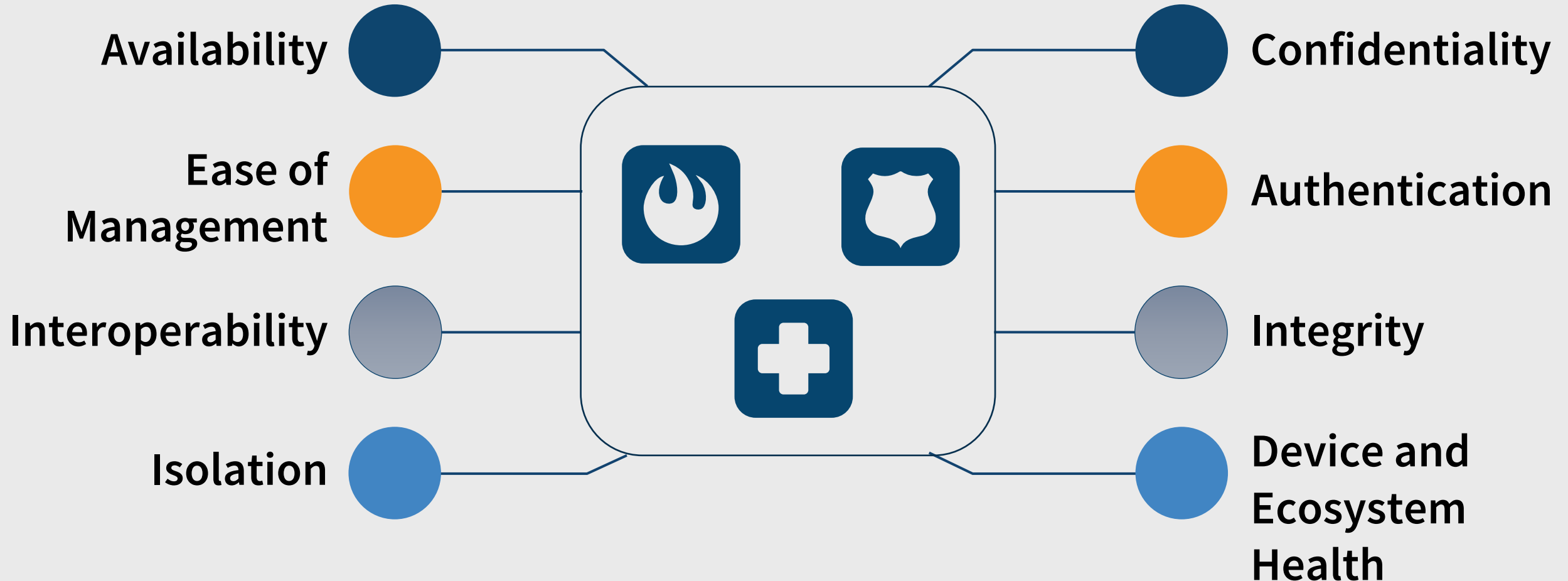
- Identify security needs for public safety devices
- Provide guidance to architect secure public safety systems

Project Outline



Public Safety Security Objectives

NISTIR 8196 - Security Analysis of First Responder Mobile and Wearable Devices



Testing Analysis

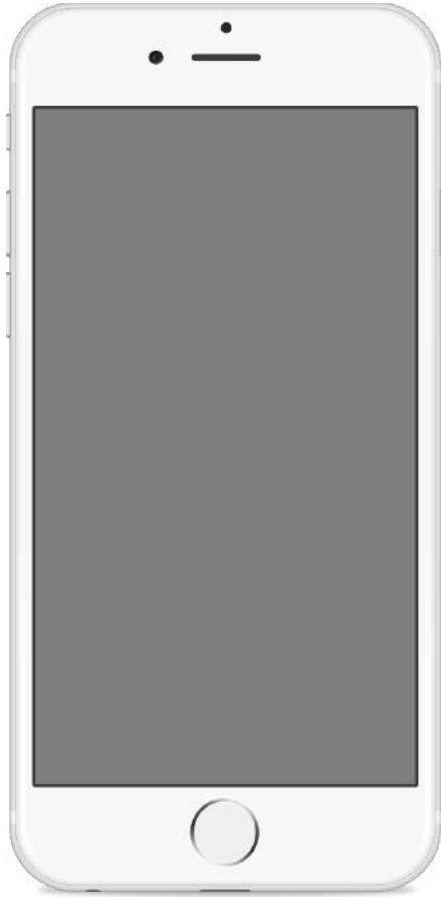
- **Purpose:**

- Understand the current security features and capabilities of public safety mobile & wearable devices

- **Methodology:**

- Develop analysis plan using the public safety security objectives
- Analyze public safety mobile and wearable devices using the analysis plan
- Identify security features, capabilities, and gaps in the technology

Mobile Device **Analysis**



Highlighted Observations:

- Easy access and **readily available device information**
 - *make, model, OS version*
- Inclusive of many **built-in security features**
 - *VPN, device encryption, authentication mechanisms*
- May receive **infrequent updates**
 - *proprietary operating system*
 - *infrequent application updates and compatibility*
- No **rogue base station detection**

Wearable Analysis



Highlighted Observations:

- **Readily available device information** but **varying** in the amount of detail
- Many did not have **a full-fledged operating system**
 - Rely on external application to process data
- **Older/outdated bluetooth version** used in all devices
 - Weak authentication process
 - Lack encryption of data
 - No MAC address randomization (susceptible to location tracking)
- **Infrequent updates** and **static device configuration**

Developing Best Practices and Guidance

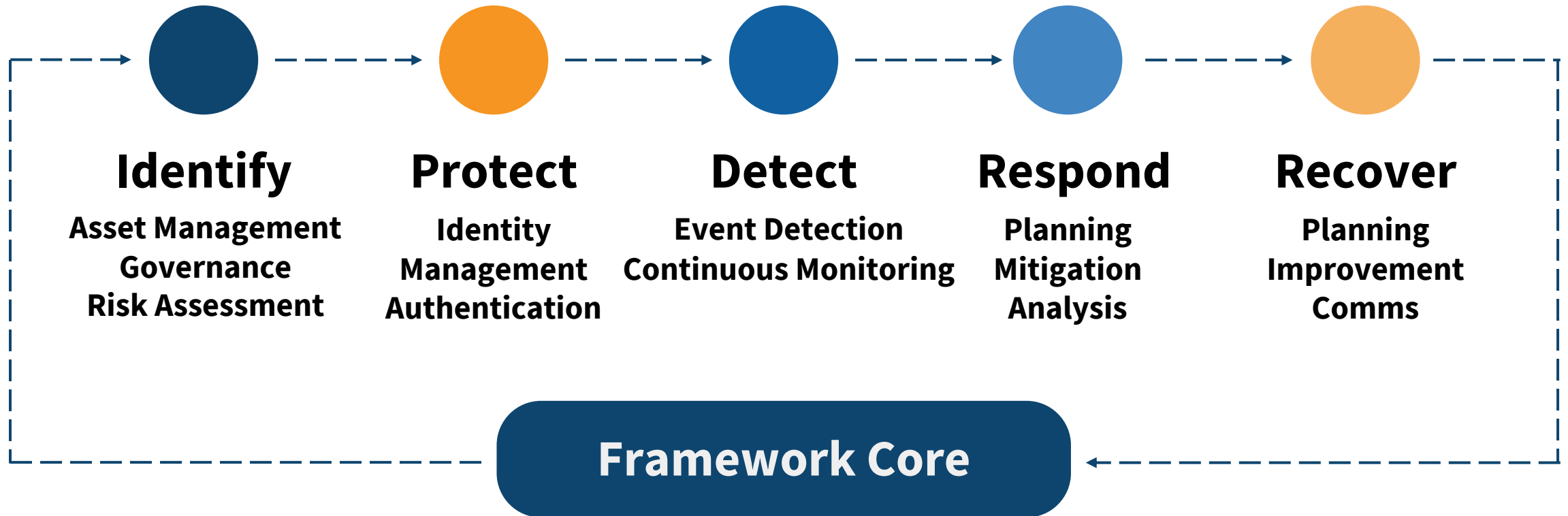
- **Purpose**

- Inform first responders of the security features necessary to achieve their security objectives
- Inform public safety device manufacturers of the security features that should be incorporated in their devices

- **Methodology**

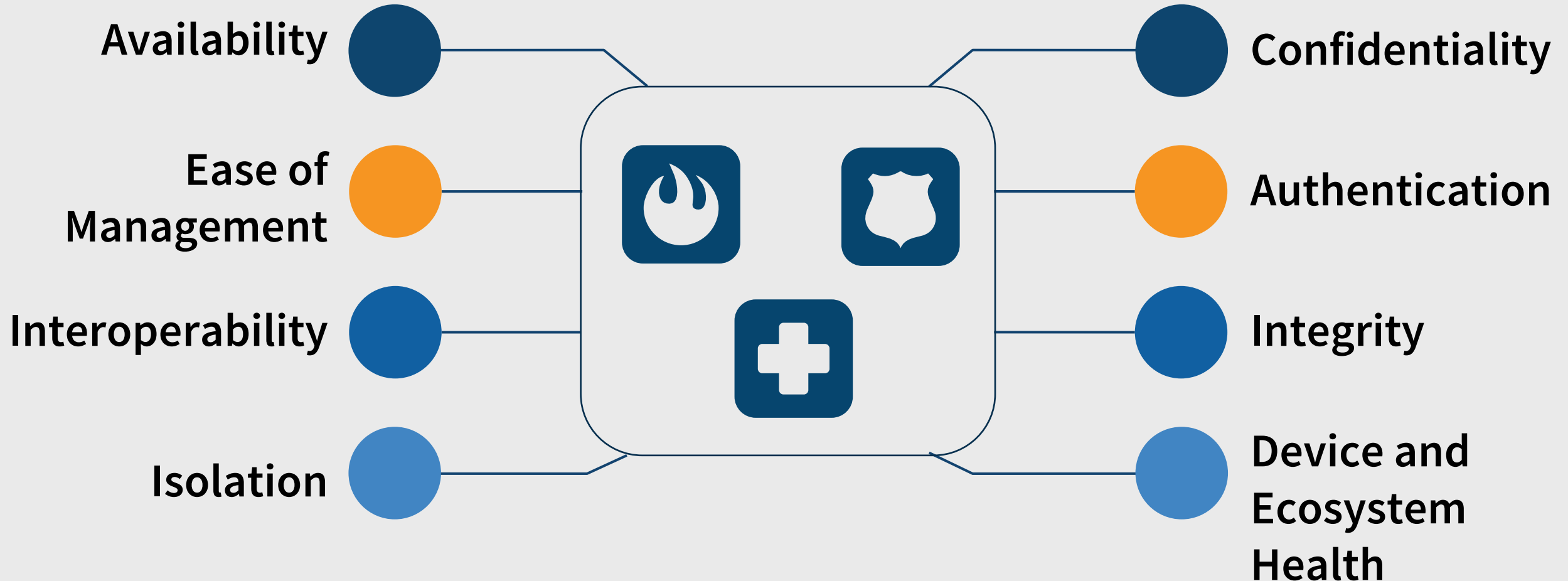
- Don't reinvent the wheel and identify relevant best practices and guidance
- Reference the NIST Cybersecurity Framework
- Reference NISTIR 8228 *Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks*

NIST Cybersecurity Framework

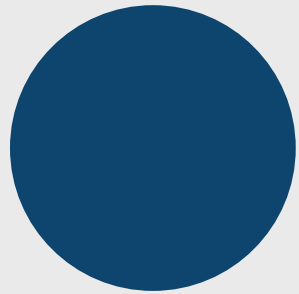


Public Safety Security Objectives

NISTIR 8196 - Security Analysis of First Responder Mobile and Wearable Devices

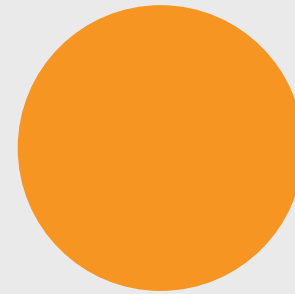


Device Guidance and Considerations



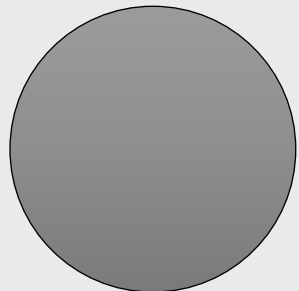
Device Awareness

Cybersecurity Framework: **Identify**
PS Security Objective: **Ease of Management**



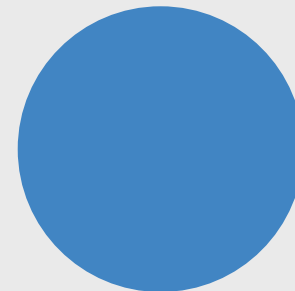
Multi-factor Authentication

Cybersecurity Framework: **Protect**
PS Security Objective: **Authentication**



Secure Boot/ Boot Validation

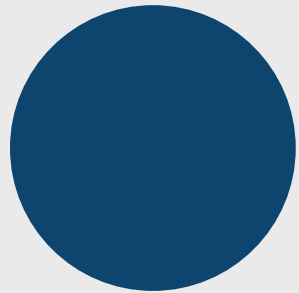
Cybersecurity Framework: **Detect**
PS Security Objective: **Integrity**



Data Isolation

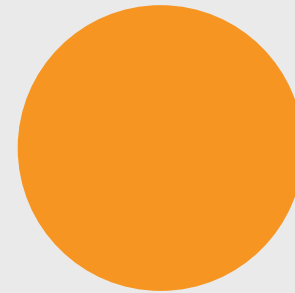
Cybersecurity Framework: **Respond**
PS Security Objective: **Isolation**

Device Guidance and Considerations



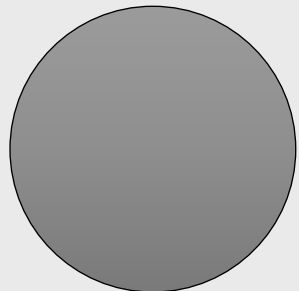
Network Interfaces Awareness

Cybersecurity Framework: **Identify**
PS Security Objective: **Ease of Management**



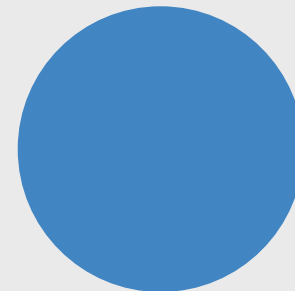
Data Encryption

Cybersecurity Framework: **Protect**
PS Security Objective: **Confidentiality**



MITM Detection

Cybersecurity Framework: **Detect**
PS Security Objective: **Integrity**

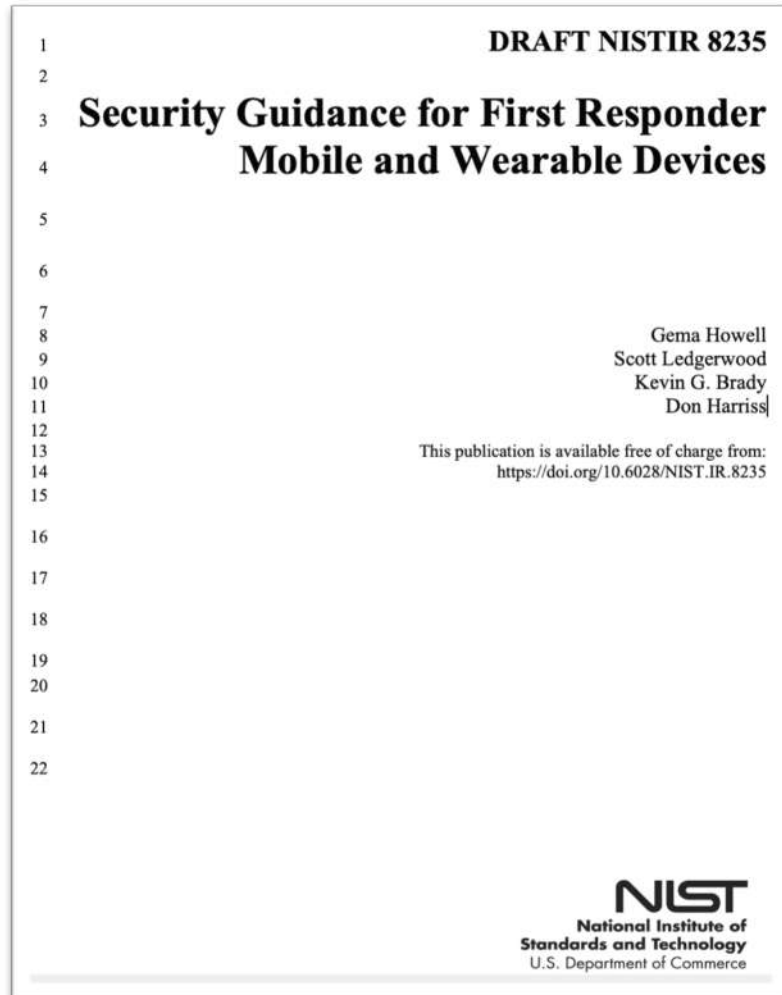


Updates and Patch Management

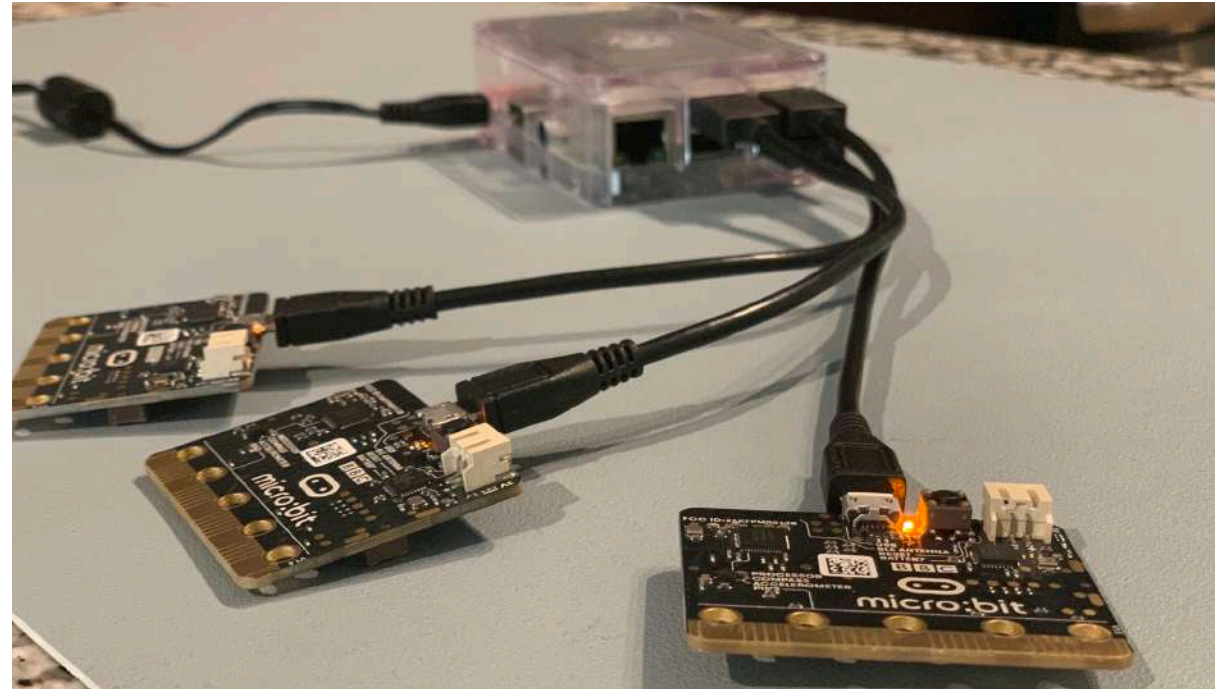
Cybersecurity Framework: **Respond**
PS Security Objective: **Device Health**

Closing Remarks

NISTIR 8235 – Security Guidance for First Responder Mobile and Wearable Devices



Demonstration of Bluetooth Attack on BLE Device

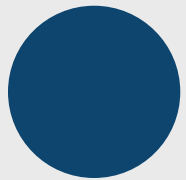


THE POWER IS YOURS!!!



THANK YOU

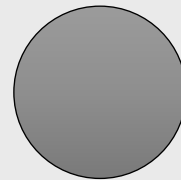
Contact The Team



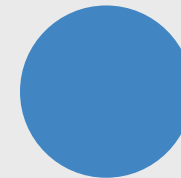
Gema Howell
Gema@nist.gov



Scott Ledgerwood
Scott.ledgerwood@nist.gov



Don Harriss
Donald.Harriss@nist.gov



Kevin G. Brady Jr.
Kevin.g.brady@nist.gov

#PSCR2019

Come back for the
**Next
Session**
1:50 PM